ADDITIVE BASES IN GROUPS

VICTOR LAMBERT, THÁI HOÀNG LÊ AND ALAIN PLAGNE

Abstract. In this paper, we study the problem of removing an element from an additive basis in a general abelian group. We introduce analogues of the classical functions X, S and E (defined in the case of $\mathbb{N}$) and obtain bounds on them. Our estimates on the functions S_G and E_G are valid for general abelian groups G while in the case of X_G we show that distinct types of behaviours may occur depending on G.

1. Introduction

1.1. **Background.** Let $(G,+)$ be an abelian semigroup. If $A \subset G$, then for h a positive integer, hA denotes as usual the h-fold sumset of A that is, the set of sums of h non-necessarily distinct elements of A. For two subsets A, B of G, we write $A \sim B$ if the symmetric difference of A and B is finite.

In this paper, we are concerned with the notion of *additive basis*. Several related notions should be defined.

We say A is an *exact asymptotic basis* (from now on, we will simply say a *basis*) of order at most h if all but finitely many elements of G can be expressed as a sum of *exactly* h elements of G, in other words, if $hA \sim G$. If h is the smallest integer for which this holds, we say that A is a basis of order h and write $\mathrm{ord}^*_G(A) = h$. If no such h exists, we write $\mathrm{ord}^*_G(A) = \infty$.

We say A is a *weak basis* of order at most h if all but finitely many elements of G can be expressed as a sum of *at most* h elements of G, in other words, if

$$\bigcup_{i=1}^{h} iA \sim G. \tag{1}$$

If h is the smallest integer for which this holds, we say that A is a weak basis of order h and write $\mathrm{ord}_G(A) = h$. If no such h exists, we write $\mathrm{ord}_G(A) = \infty$.

Finally, a basis A of order at most h is called *nice* if $hA = G$. A weak basis A of order at most h is called *nice* if (1) is in fact an equality.

These notions are related by the following simple observation. Assume that the ambient semigroup G contains the neutral element 0. Then A is a weak basis if and only if $A \cup \{0\}$ is a basis. Furthermore, $\mathrm{ord}_G(A) = \mathrm{ord}^*_G(A \cup \{0\})$. (Weak) bases are of interest only when G is infinite. On the other hand, nice (weak) bases make sense in any semigroup.

Date: August 12, 2015.

Historically, additive bases have been studied in the case where $G = \mathbb{N}$, the semigroup of nonnegative integers. In the fundamental paper [3], Erdős and Graham studied the following problem (note that the original formulation of Erdős and Graham is slightly different, but equivalent, see Section 2.2): let $A \subset \mathbb{N}$ be a basis and $a \in A$, when is $A \setminus \{a\}$ a basis? If $A \setminus \{a\}$ is still a basis, what can we say about its order? Since then, this question and related questions have been extensively studied. We give here a brief survey of state-of-the-art results in this theme of research. For more detailed accounts, we refer the reader to [12] or [5].

It turns out that there are only finitely many elements $a \in A$ such that $A \setminus \{a\}$ is not a basis, which we refer to as *exceptional* elements. An element $a \in A$ which is not exceptional is called *regular*. Let A^* denote the set of all regular elements of A. Grekos [6] showed that the number of exceptional elements of A can be bounded in terms of h alone, thus we can define the function

$$E(h) = \max_{hA \sim \mathbb{N}} |A \setminus A^*|. \tag{2}$$

By the third author's work [14], we have the following asymptotic formula as $h \to \infty$:

$$E(h) \sim 2\sqrt{\frac{h}{\log h}}. \tag{3}$$

Erdős and Graham [3] showed that when a is regular, the order of $A \setminus \{a\}$ can be bounded in terms of h alone. Thus we can define the function

$$X(h) = \max_{hA \sim \mathbb{N}} \max_{a \in A^*} \operatorname{ord}^*(A \setminus \{a\}). \tag{4}$$

To date, the best upper and lower bounds for $X(h)$ are both due to the third author [13], improving earlier works by Stöhr [15], Grekos [6] and Nash [11] notably. We have

$$\left\lceil \frac{h(h+4)}{3} \right\rceil \leq X(h) \leq \frac{h(h+1)}{2} + \left\lceil \frac{h-1}{3} \right\rceil. \tag{5}$$

It is conjectured by Erdős and Graham [4] that there is a constant α such that $X(h) \sim \alpha h^2$ as $h \to \infty$, but this remains open. The inequalities in (5) imply that $X(1) = 1, X(2) = 4$, $X(3) = 7$, but even the value of $X(4)$ remains unknown.

In [6, 7], Grekos observed that in examples of bases A of order h that give large values of $X(h)$, there are actually very few elements $a \in A$ such that $\operatorname{ord}^*(A \setminus \{a\}) = X(h)$. This led him to introduce the function

$$S(h) = \max_{hA \sim \mathbb{N}} \limsup_{a \in A^*} \operatorname{ord}^*(A \setminus \{a\}) \tag{6}$$

and to conjecture that the order of magnitude of S is smaller than the one of X. This was confirmed by Cassaigne and the third author [3] who proved that

$$h + 1 \leq S(h) \leq 2h \tag{7}$$

for all $h \geq 2$ (evidently, $S(1) = 1$). It was also determined that $S(2) = 3$. However, the value of $S(3)$ is still unknown. It is an open problem which looks already difficult to determine whether there is a constant β such that $S(h) \sim \beta h$ as $h \to \infty$.

1.2. **Our work.** The goal of this paper is to study the analogues of the functions E, X, S defined above when G is an arbitrary infinite abelian group. Clearly, this problem makes sense in any semigroup. However, the rich structure of a group gives us more tools and flexibility. As such, our results are not generalizations of results in $\mathbb{N}$, but rather their analogues. Indeed, many of the results in $\mathbb{N}$ do not apply automatically to $\mathbb{Z}$, and vice versa.

Before studying the problem of removing elements from a basis in a group G, it is quite natural to ask if G has any basis of order ≥ 2 at all. We will show that not only has G a basis, but it also has a *minimal basis* of any prescribed order. A basis A of order h of G is called minimal if for any $a \in A$, $A \setminus \{a\}$ is no longer a basis of order h (it could be a basis of some larger order). In other words, any element of A is necessary in order for A to be a basis of order h. This result is the content of our first theorem.

Theorem 1. *Let G be any infinite abelian group and h be an integer, $h \geq 2$. Then G has a nice minimal basis of order h.*

We can now talk about the analogues of the functions E, X, S defined on $\mathbb{N}$. Let A be a basis of G. An element $a \in A$ is called *exceptional* if $A \setminus \{a\}$ is not a basis of G of any order, and *regular* if it is not exceptional. Let A^* be the set of regular elements of A. We show that similarly to the case of $\mathbb{N}$, there are only finitely many exceptional elements in A. More precisely, define

$$E_G(h) = \max_{hA \sim G} |A \setminus A^*|$$

A priori, it is not clear that this function is well-defined (i.e., the number of exceptional elements of A can be bounded in terms of h alone). However, we will prove the following result.

Theorem 2. *(i) For any infinite abelian group G and any integer $h \geq 2$, we have*

$$E_G(h) \leq h - 1.$$

(ii) There is an infinite group G, for which $E_G(h) = h - 1$ for any integer $h \geq 2$.

(iii) For each integer $h \geq 2$, there is an infinite group G (depending on h) for which $E_G(h) = 0$.

The statements (ii) and (iii) in this theorem show that, as far as general groups are concerned, the upper bound (i) is the best possible one can hope for. Also, it is easy to see that $E_G(1) = 0$ for any G.

Next we turn to the question of bounding the order of $A \setminus \{a\}$ when $a \in A$ is a regular element. Define

$$X_G(h) = \max_{hA \sim G} \max_{a \in A^*} \operatorname{ord}^*_G(A \setminus \{a\}). \tag{8}$$

Studying the function X_G turns out to be less successful than E_G. We do not even know if $X_G(h)$ is finite for each G, not to mention the problem of proving that $X_G(h)$ can be bounded in terms of h alone. However, in the case of some particular groups we are able to prove bounds for $X_G(h)$.

In order to state our next result, we shall need the arithmetic function Ω. Recall that it is defined by

$$\Omega(n) = \alpha_1 + \cdots + \alpha_k, \tag{9}$$

if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ is the prime factorization of n.

Another notation that we shall need is for A a subset of a group G and m an integer

$$m \cdot A = \{ma : a \in A\}.$$

By adapting Erdős-Graham's argument from [3], we prove the following statement.

Theorem 3. *Let G be an infinite abelian group. If for any integer $1 \leq m \leq h$, the quotient group $G/m \cdot G$ is finite then we have*

$$X_G(h) \leq h^2 + h \cdot \max_{1 \leq m \leq h} \Omega\left(|G/m \cdot G|\right) + h - 1. \tag{10}$$

Groups that satisfy the hypothesis of Theorem 3 include large classes such as finitely generated groups, divisible groups (i.e., groups G such that $m \cdot G = G$ for all $m \in \mathbb{Z}^+$, which include $\mathbb{R}$ and $\mathbb{Q}$) and $\mathbb{Z}_p$ (the p-adic integers).

As for lower bounds, the same as in (5) applies to groups which have $\mathbb{Z}$ as a quotient. That is, we can prove the following.

Theorem 4. *Let G be an infinite abelian group. Suppose there is a subgroup H of G such that $G/H \cong \mathbb{Z}$, then for any integer $h \geq 1$, we have*

$$X_G(h) \geq \left\lfloor \frac{h(h+4)}{3} \right\rfloor.$$

This prompts one to believe that the growth of $X_G(h)$ in general is quadratic. However, we show that this is not the case by exhibiting another class of groups for which $X_G(h)$ has a *linear* growth.

Theorem 5. *Let p be a prime number and G be an infinite abelian group with the property that every nonzero element of G has order p.*

(i) For any integer $h \geq p$, we have

$$X_G(h) \leq ph + p - 1.$$

(ii) For any integer $h \geq 3(p-1)/2$, we have

$$X_G(h) \geq 2h - 3p + 3.$$

In particular, if $p = 2$, then $X_G(h) \sim 2h$ as $h \to \infty$.

Though in general we do not know if $X_G(h)$ is finite, we can confirm this when $h = 2$ or $h = 3$ (for any infinite abelian group G). Clearly, $X_G(1) = 1$.

Theorem 6. *For any infinite abelian group G, we have*

(i) $3 \leq X_G(2) \leq 5$.
(ii) $4 \leq X_G(3) \leq 17$.

Finally, we turn to the analogue of S. We define $S_G(h)$ to be the minimum value of s such that for all A satisfying $hA \sim G$, there are only finitely many elements $a \in A$ with the property that

$$\mathrm{ord}_G^*(A \setminus \{a\}) > s.$$

Again, a priori, it is not clear that $S_G(h)$ is well defined (though it is clear that $S_G(1) = 1$ for any G). It follows immediately from the definition that $S_G(h) \leq X_G(h)$. We show that for $S_G(h)$, we have exactly the same bounds as in (7), by generalizing the arguments from [2]. In doing so, we need to use the notion of *amenability*, which makes the argument no longer elementary.

Theorem 7. *For any infinite abelian group G and $h \geq 2$, we have $h + 1 \leq S_G(h) \leq 2h$.*

In contrast with Theorem 2 but as in the case of $\mathbb{N}$, we do not know if these bounds are best possible. However, we can prove the following equality.

Theorem 8. *For any infinite abelian group G, we have $S_G(2) = 3$.*

The structure of the paper is as follows. In Section 2, we will prove some useful facts, including a generalization of the Erdős-Graham's criterion for regular elements of a basis. In Section 3, we will prove Theorem 1. In Section 4, we will prove results related to the function E_G, including Theorem 2. In Section 5, we will prove results related to the function X_G, including Theorems 3, 4, 5 and 6. Finally, we will prove results related to the function S_G, including Theorems 7 and 8 in Section 6.

2. Preliminaries

2.1. **Some observations.** We first state some simple observations which we will use later on. Some of them are immediate and the proofs will be omitted.

Lemma 1. *Let G be an infinite abelian group and $A \subset G$. If A is a (nice) basis of G and $b \in G$, then $A - b = \{a - b : a \in A\}$ is a (nice) basis of the same order.*

Proof. This is immediate since, for any integer h, $h(A - b) = hA - hb$. □

Suppose H is a subgroup of G. For $x \in G$, let $\overline{x}$ denote the coset of x in G/H (we distinguish between elements of G/H and subsets of G). Then there is a natural way to produce a basis for G.

Lemma 2. *Let G be an abelian group and H be a subgroup of G. Let $\Lambda \subset G$ be a system of representatives of G/H in G, that is, for any $x \in G$, there is exactly one element $\lambda \in \Lambda$ such that $x + H = \lambda + H$. Then every $x \in G$ can be expressed in a unique way as*

$$x = \lambda + g$$

where $\lambda \in \Lambda, g \in H$. In particular, if $H \neq G$ and $H \neq \{0\}$ then $\Lambda \cup H$ is a nice basis of order 2 of G.

In constructing bases for G we will need special systems of representatives which are given by the following

Lemma 3. *Let G be an abelian group and H be a subgroup of G. Then there is a system of representatives Λ of G/H in G such that $0 \in \Lambda$ and $\Lambda = -\Lambda$.*

Proof. We select one representative from each coset of H in G. Of course, we can select in such a way that 0 is the representative of H, and if λ is the representative of a coset B, then $-\lambda$ is the representative of the coset $-B$. □

The next observation says that nice bases can be lifted from quotients to the whole group, a property not satisfied by mere bases.

Lemma 4. *Let G be an infinite abelian group and H be a subgroup of G. Let $A \subset G/H$,*

$$B = \{x \in G : \overline{x} \in A\}$$

and h be a positive integer. Then we have:

(i) $hA = G/H$ if and only if $hB = G$,
(ii) $\bigcup_{i=1}^{h} iA = G/H$ if and only if $\bigcup_{i=1}^{h} iB = G$.

The next lemma says that all bases are nice, at the cost of increasing the order.

Lemma 5. *Let G be an infinite abelian group and $A \subset G$.*

(i) If $hA \sim G$, then $(h+1)A = G$,
(ii) If $\bigcup_{i=1}^{h} iA \sim G$, then $\bigcup_{i=2}^{h+1} iA = G$.

Proof. Suppose $hA \sim G$. Let x be any element of G. Then $x - A$ is infinite, so it must have a non-empty intersection with hA. Therefore, $x \in (h+1)A$.

Suppose $\bigcup_{i=1}^{h} iA \sim G$. Let x be any element of G. Since $x - A$ is infinite, it must have a non-empty intersection with rA for some $1 \leq r \leq h$. Therefore,

$$x \in (r+1)A \subset \bigcup_{i=2}^{h+1} iA.$$

□

In finding bounds for X_G, we will need the following fact. If two sumsets of A have a non-empty intersection, then we can find an arbitrarily long sequence of sumsets of A whose intersection is also non-empty.

Lemma 6. *Suppose $A \subset G$ and m, n be nonnegative integers. If*

$$c \in nA \cap (n+m)A$$

then for any positive integer k, we have

$$kc \in knA \cap (kn+m)A \cap \cdots \cap (kn+km)A.$$

2.2. **Erdős-Graham type criteria.** In [3], Erdős and Graham proved a criterion for weak bases in $\mathbb{N}$. They show that a weak basis A of $\mathbb{N}$ is a basis if and only if

$$\gcd(A - A) = 1 \tag{11}$$

where $A - A = \{a_1 - a_2 : a_1, a_2 \in A\}$. In turn, this implies a criterion for regular elements of a basis in $\mathbb{N}$. If A is a basis of $\mathbb{N}$, then $a \in A$ is regular if and only if

$$\gcd(A \setminus \{a\} - A \setminus \{a\}) = 1. \tag{12}$$

We will now prove extensions of these criteria in an arbitrary group.

Lemma 7. *Let G be an infinite abelian group and A be a weak basis of G. Then A is a basis if and only if $\langle A - A\rangle$, the group generated by $A - A$ in G, is equal to G.*

Proof. Suppose A is a weak basis of order at most h, that is,

$$G \sim \bigcup_{i=1}^{h} iA.$$

Let $H = \langle A - A\rangle$. The image of a in G/H is the same, for any $a \in A$. Therefore, for any s, the image of sA in G/H consists of a single element. This means that A cannot be a basis unless $G = H$.

Conversely, suppose $G = H$. We claim that there is a positive integer n such that

$$nA \cap (n+1)A \neq \emptyset.$$

Let a be any element of A. Then a can be expressed as a linear combination

$$a = \sum_{k=1}^{t} \alpha_k (a_k - b_k)$$

where $a_k, b_k \in A$ and $\alpha_k \in \mathbb{Z}^+$ for any index k.

Hence the element

$$c = a + \sum_{k=1}^{t} \alpha_k b_k = \sum_{k=1}^{t} \alpha_k a_k$$

is in both nA and $(n+1)A$, where $n = \sum_{k=1}^{t} \alpha_k$. By Lemma 6, we have

$$(h-1)c \in \bigcap_{i=0}^{h-1} ((h-1)n + i)A.$$

For all but finitely many $x \in G$, we have

$$x - (h-1)c \in \bigcup_{i=1}^{h} iA.$$

It follows that for all but finitely many $x \in G$, we have

$$x = x - (h-1)c + (h-1)c \in ((h-1)n + h)A.$$

Thus A is a basis with order $\leq (h-1)n + h$. □

Lemma 8. *Let G be an infinite abelian group and A be a basis of G. Then $a \in A$ is regular if and only if $\langle A \setminus \{a\} - A \setminus \{a\}\rangle = G$.*

Proof. We want to apply Lemma 7 right away, but we do not know if $A \setminus \{a\}$ is a weak basis. Instead, we observe that $B := A - a$ is also a basis, and contains 0. Therefore, $B \setminus \{0\}$ is a weak basis. We have

$$\begin{aligned} A \setminus \{a\} \text{ is a basis} &\iff B \setminus \{0\} \text{ is a basis} \\ &\iff \langle B \setminus \{0\} - B \setminus \{0\} \rangle = G \\ &\iff \langle A \setminus \{a\} - A \setminus \{a\} \rangle = G. \end{aligned}$$

□

In [3], Erdős and Graham gave a slightly different but equivalent definition of the function X. We will revisit their original definition since we find it convenient to work with both definitions. If G is an infinite abelian group, we define

$$\begin{aligned} x_G(h) &= \max\{\mathrm{ord}^*_G(A) : \cup_{i=1}^h iA \sim G \text{ and } \mathrm{ord}^*_G(A) < \infty\} \\ &= \max\{\mathrm{ord}^*_G(A) : \cup_{i=1}^h iA \sim G \text{ and } \langle A - A \rangle = G\}. \end{aligned} \tag{13}$$

Lemma 9. *For every infinite abelian group G, $X_G = x_G$.*

Proof. Let h be a positive integer, A be any basis of order at most h of G and $a \in A$ be any regular element of A. Then $B := A - a$ is also a basis of order at most h and contains 0. Therefore, $B \setminus \{0\}$ is a weak basis of order at most h. Furthermore,

$$\mathrm{ord}^*_G(B \setminus \{0\}) = \mathrm{ord}^*_G(A \setminus \{a\}).$$

This implies that $X_G(h) \leq x_G(h)$.

The other direction is a bit less straightforward. From the definitions of X and x, clearly we have $h \leq X_G(h)$ and $h \leq x_G(h)$. If $x_G(h) = h$ then necessarily $X_G(h) = h = x_G(h)$, since we already know $X_G(h) \leq x_G(h)$. Thus we may assume that $x_G(h) > h$ (we notice that in view of Theorem 1, which is yet to be proved, this is always the case if $h \geq 2$). Let B be any weak basis of order at most h of G satisfying $h < \mathrm{ord}^*_G(B) < \infty$. Then $0 \notin B$ (if not, $\mathrm{ord}^*_G(B) = \mathrm{ord}_G(B) \leq h$). Let $A := B \cup \{0\}$, then A is a basis of order at most h and 0 is a regular element of A, since $A \setminus \{0\} = B$. Furthermore,

$$\mathrm{ord}^*_G(A \setminus \{0\}) = \mathrm{ord}^*_G(B).$$

This implies that $x_G(h) \leq X_G(h)$. □

3. Existence of minimal bases

In the case of $\mathbb{N}$, it has been known since Härtter [9] that $\mathbb{N}$ has minimal bases of any order (though his proof is non-constructive). A concrete example of a minimal basis of order h in $\mathbb{N}$ is given by

$$A = \left\{ \sum_{f \in \mathcal{F}} 2^f : \mathcal{F} \text{ is a finite set of distinct nonnegative integers congruent modulo } h \right\}.$$

See [10] for further quantitative properties of this basis.

We first show that in a general group G, there are nice bases of any order as long as there is a special representation of elements of G similar to base 2 representation.

Proposition 1. *Let G be an infinite abelian group. Suppose that there is an infinite sequence of subsets $(\Lambda_i)_{i=0}^{\infty}$ of G satisfying the following properties:*

(i) $0 \in \Lambda_i$, *for any* $i \in \mathbb{N}$,
(ii) $-\Lambda_i = \Lambda_i$, *for any* $i \in \mathbb{N}$,
(iii) Every element $x \in G$ *has a* unique *representation as*

$$x = \lambda_0(x) + \lambda_1(x) + \cdots$$

where $\lambda_i(x) \in \Lambda_i$ *for any* i, *and* $\lambda_i(x) = 0$ *for all but finitely many indices* i. *In other words,* G *is equal to the "direct sum"* $\oplus_{i=0}^{\infty}\Lambda_i$. [1]

Then for any integer $h \geq 2$, G *has a nice minimal basis of order* h.

Proof. For $x \in G$, we refer to the set $\{i \in \mathbb{N} : \lambda_i(x) \neq 0\}$ as the *support* of x.

Clearly, if x and y have disjoint supports, then

$$\lambda_i(x+y) = \lambda_i(x) + \lambda_i(y).$$

Let $\mathbb{N} = N_1 \cup \cdots \cup N_h$ be a partition of $\mathbb{N}$ into h infinite disjoint sets. Let A_j be the set of all $x \in G$ supported on N_j. Put

$$A = \cup_{j=1}^{h} A_j.$$

By definition, $0 \in A$. Clearly, any element $x \in G$ can be expressed in a *unique* way as

$$x = a_1 + \cdots + a_h \tag{14}$$

where $a_j \in A_j$ for any $j = 1, \ldots, h$. When $a_1, \ldots, a_h \neq 0$, x cannot be written as a sum of fewer than h elements from A. This shows that A is a basis of order h. However, A is not minimal. We claim that $B := A \setminus \{0\}$ is a nice, minimal basis of order h.

First we show that $hB = G$. In the expression (14), some (or even all) of the a_j can be 0. We now observe that any (zero or non-zero) element in A_j can be expressed as a sum of two *non-zero* elements of A_j. Indeed, if $a \in A_j$, then a can be written as

$$a = (a + \lambda) + (-\lambda)$$

where λ is any element in $\Lambda_k \setminus \{0\}$ and $k \in N_j$ is any element not in the support of a. Note that by hypothesis, $-\lambda \in \Lambda_k$ as well. Thus starting from (14) we can increase the number of non-zero elements by one at a time, which shows that $hB = G$.

It remains to see that B is a minimal basis. Let a be any element in B. Without loss of generality, we may assume $a \in A_1 \setminus \{0\}$. Consider an element $x \in G$ of the form

$$x = a + a_2 + \cdots + a_h$$

where $a_j \in A_j \setminus \{0\}$ for any $j = 2, \ldots, h$. Then there is a unique way to write x as a sum of h elements of B, and a appears in this expression. Therefore, x cannot be written as a sum of h elements from $B \setminus \{a\}$. Since there are infinitely many elements x of this form, it follows that $\mathrm{ord}^*(A \setminus \{a\}) \geq h + 1$. □

The proof of Theorem 1 now follows.

[1] Strictly speaking, we cannot talk about direct sums here since the Λ_i are merely sets, not groups.

Proof of Theorem 1. It suffices to construct a sequence $(\Lambda_i)_{i=0}^{\infty}$ satisfying the hypothesis of Proposition 1. We distinguish two cases.

Case 1: G has an element of infinite order. We may assume that $\mathbb{Z} < G$. Let Λ_0 be a system of representatives of $G/\mathbb{Z}$ in G. By Lemma 2, any element $x \in G$ can be written in a unique way as

$$x = n + \lambda_0$$

where $\lambda_0 \in \Lambda_0$ and $n \in \mathbb{Z}$. Furthermore, by Lemma 3, we may choose Λ_0 in such a way that $0 \in \Lambda_0$ and $\Lambda_0 = -\Lambda_0$. Observe that every integer n can be written in a *unique* way as

$$n = \sum_{i=0}^{k} a_i 3^i$$

where $a_i \in \{0, 1, -1\}$ for any i (this is known in the literature as the *balanced ternary* representation of n). Put $\Lambda_i = \{0, 3^{i-1}, -3^{i-1}\}$. Then any element $x \in G$ can be written in a unique way as

$$x = \lambda_0(x) + \lambda_1(x) + \cdots \tag{15}$$

where $\lambda_i(x) \in \Lambda_i$ for any i, and $\lambda_i(x) = 0$ for all but finitely many indices i.

Case 2: Every element of G has finite order.

Let $g_1 \in G$ be any element. Then $G_1 := \langle g_1 \rangle$ is finite. We can find $g_2 \in G \setminus G_1$. Put $G_2 := \langle g_1, g_2 \rangle$, then $G_1 \lneq G_2$ and G_2 is finite. This way, we have an infinite chain of subgroups of G

$$G_1 \lneq G_2 \lneq \cdots .$$

For each integer $i \geq 2$, let $\Lambda_i \ni 0$ be a system of representatives of G_i/G_{i-1} in G_i. By Lemma 2, any $x \in G_i$ can be written in a unique way as

$$x = \lambda + g$$

where $\lambda \in \Lambda_i$ and $g \in G_{i-1}$. We also put $\Lambda_1 = G_1$. Thus every $x \in \cup_{i=1}^{\infty} G_i$ can be written in a unique way as

$$x = \lambda_1(x) + \lambda_2(x) + \cdots$$

where $\lambda_i \in \Lambda_i$ for any $i = 1, 2, \ldots$, and all but finitely many λ_i are zero (indeed, if $x \in G_k$, then $\lambda_i(x) = 0$ for all $i \geq k + 1$).

Finally, let $\Lambda_0 \ni 0$ be a system of representatives of $G/\cup_{i=1}^{\infty} G_i$ in G. Then every x in G can be written in a unique way as

$$x = \lambda_0(x) + \lambda_1(x) + \lambda_2(x) + \cdots$$

where $\lambda_i \in \Lambda_i$ for any $i = 0, 1, 2, \ldots$, and all but finitely many λ_i are zero. Furthermore, by Lemma 3, we may require that $\Lambda_i = -\Lambda_i$ for $i = 0$ and any $i \geq 2$ (this is certainly satisfied when $i = 1$). □

4. The function E_G

In this section, we study bounds for E_G.

Proof of Theorem 2 (i). We will show that if $hA \sim G$, then A cannot have more than $h-1$ exceptional elements.

By Lemma 8, if a is an exceptional element, then $\langle A - A\rangle = G$ but $\langle A\setminus\{a\} - A\setminus\{a\}\rangle \neq G$. This implies that $a-a'$ is not in $\langle A\setminus\{a\} - A\setminus\{a\}\rangle$ for *some* (and hence for *all*) $a' \in A\setminus\{a\}$.

Suppose there are at least h exceptional elements $a_1, \dots, a_h$ in A. Since G is infinite, so is A. Let a_0 be an element in $A\setminus\{a_1, \dots, a_h\}$. Since $hA \sim G$, we can find $a \in A\setminus\{a_0, a_1, \dots, a_h\}$ such that the element

$$a_0 + a_1 + a_2 + \cdots + a_h - a$$

can be expressed as a sum $b_1 + \cdots + b_h$ of h elements in A. Therefore,

$$\sum_{i=0}^{h}(a_i - a) = \sum_{i=1}^{h}(b_i - a).$$

Some of the b_i may be equal to some of the a_i. We have two possibilities.

Case 1: $\{a_1, a_2, \dots, a_h\} \neq \{b_1, b_2, \dots, b_h\}$. This means that after canceling common terms, some a_i (where $i \neq 0$) must remain on the left hand side. But this implies that $a_i - a \in \langle A\setminus\{a_i\} - A\setminus\{a_i\}\rangle$, a contradiction.

Case 2: $\{a_1, a_2, \dots, a_h\} = \{b_1, b_2, \dots, b_h\}$. This implies that $a_0 = a$, a contradiction. □

A remark should be made here. In $\mathbb{N}$, the fact that any basis has only finitely many exceptional elements follows immediately from Erdős-Graham's criterion (11) (see [12, Teorema 1]). However, that proof relies on a special property of $\mathbb{Z}$, namely that all strictly increasing sequences of subgroups of $\mathbb{Z}$ are finite. As such, it cannot be generalized to general groups.

Theorem 2 (ii) and (iii) follow immediately from the following proposition.

Proposition 2. *Let $G = \mathbb{F}_p[t]$ be the ring of polynomials over a prime field $\mathbb{F}_p$. For any integer $h \geq 2$, we have*

$$E_G(h) = \left\lceil \frac{h-1}{p-1} \right\rceil.$$

In particular, if $p = 2$ then $E_G(h) = h - 1$ for all $h \geq 2$. On the other hand, there is no non-trivial universal lower bound for $E_G(h)$, since $E_G(h) = 0$ when $p > h$.

Proof. First we show that

$$E_G(h) \leq \left\lceil \frac{h-1}{p-1} \right\rceil.$$

We argue similarly to the proof of Theorem 2 (i).

Suppose $A \subset \mathbb{F}_p[t]$ is a basis of order h, and $a_1, \dots, a_k$ are all the exceptional elements of A. Suppose for a contradiction that $k(p-1) \geq h$. Then there exists $0 \leq \alpha_1, \dots, \alpha_k \leq p-1$ such that

$$\alpha_1 + \cdots + \alpha_k = h.$$

Let a_0 be another element in $A \setminus \{a_1, \dots, a_k\}$. Since $hA \sim G$ and A is infinite, there is $a \in A \setminus \{a_0, a_1, \dots, a_k\}$ such that the element

$$\sum_{i=1}^{k} \alpha_i a_i + a_0 - a$$

can be expressed as a sum $\sum_{j=1}^{h} b_i$ of h elements of A. Therefore,

$$\sum_{i=1}^{k} \alpha_i (a_i - a) + (a_0 - a) = \sum_{j=1}^{h} (b_i - a).$$

Since $a_0 - a \neq 0$, the multisets $\{a_1(\alpha_1 \text{ times}), \dots, a_k(\alpha_k \text{ times})\}$ and $\{b_1, \dots, b_h\}$ are distinct. Therefore, after canceling common terms, there is $1 \leq i \leq k$ and some $0 < \beta \leq \alpha_i$ such that $\beta(a_i - a)$ lies in $\langle A \setminus \{a_i\} - A \setminus \{a_i\} \rangle$. This in turn implies that $a_i - a$ lies in this subspace as well (here we are using the fact that $\mathbb{F}_p$ is a field!), which contradicts Lemma 8 since a_i is exceptional.

Therefore, $h - 1 \geq (p-1)k$ and consequently $k \leq [(h-1)/(p-1)]$.

The following simple example shows that equality is attained. Let

$$k = \left[\frac{h-1}{p-1} \right].$$

Perform the Euclidean division $h = k(p-1) + r + 1$ where $0 \leq r < p - 1$.

Let

$$A = \left\{ 1, t, \cdots, t^{k-1} \right\} \bigcup t^k \cdot \mathbb{F}_p \bigcup \cdots \bigcup t^{k+r-1} \cdot \mathbb{F}_p \bigcup t^{k+r} \cdot \mathbb{F}_p[t].$$

(The sets $t^k \cdot \mathbb{F}_p, \dots, t^{k+r-1} \cdot \mathbb{F}_p$ are not there if $r = 0$.)

Then A is a basis of order $k(p-1) + r + 1 = h$. Indeed, it is easy to see that all elements in $\mathbb{F}_p[t]$ can be expressed as a sum of $k(p-1) + r + 1$ elements from A (note that $0 \in A$). Furthermore, for all $P(t) \in \mathbb{F}[t] \setminus \{0\}$, the element

$$\sum_{i=0}^{k-1} (p-1) t^i + \sum_{i=k}^{k+r-1} t^i + P(t) t^{k+r}$$

cannot be expressed as a sum of fewer than h elements from A.

Using Lemma 8, it is easy to see that the exceptional elements in A are exactly

$$\left\{ t^i : i = 0, \dots, k-1 \right\}.$$

□

5. The function X_G

In this section, we study bounds for X_G. We remind the reader that we will use freely both definitions for X_G, namely (8) and (13) which coincide by Lemma 9.

5.1. **General bounds.** In proving Theorem 3, we will need the following (recall that the function Ω is defined in (9)).

Lemma 10. *Let G be a finite abelian group which is m-torsion (that is, $mx = 0$ for all $x \in G$). Let $A \subset G$ satisfy $\langle A - A\rangle = G$. Then for any integer $s \geq \Omega(|G|)$, we have $smA = G$.*

Proof. Since $\langle A - A\rangle = G$, we can choose elements $a_1, a_2, \ldots$ of A in such a way that for any integer k, if $\langle A_k - A_k\rangle \neq G$, then $\langle A_k - A_k\rangle \lneq \langle A_{k+1} - A_{k+1}\rangle$, where

$$A_k = \{a_1, \ldots, a_k\}.$$

It is easy to see that any strictly increasing sequence of subgroups of G has length at most $\Omega(|G|)$. Hence for some integer $t \leq \Omega(|G|)$, we have $\langle A_t - A_t\rangle = G$. Thus every element $x \in G$ has a representation

$$x = \sum_{i,j=1}^{t} \alpha_{i,j}(a_i - a_j)$$

where $\alpha_{i,j} \in \mathbb{Z}$. By rearranging the right-hand side, and since G is m-torsion, this implies that we have a representation

$$x = \sum_{i}^{t} \beta_i a_i$$

where $0 \leq \beta_i < m$ for any $i = 1, \ldots, t$ and $\sum_{i=1}^{t} \beta_i$ is a multiple of m. Since $0 \in mA$, we can add as many zeroes as we want and have $x \in tmA \subset smA$, as desired. □

Proof of Theorem 3. We use the definition (13). Let A be a weak basis of order at most h of G satisfying $\langle A - A\rangle = G$. Let

$$s = \max_{1 \leq m \leq h} \Omega\left(|G/m \cdot G|\right).$$

Since $(h+1)A \subset G \sim \bigcup_{i=1}^{h} iA$, there must be some integer n satisfying $1 \leq n \leq h$ such that $nA \cap (h+1)A \neq \emptyset$.

Let $m = h + 1 - n$ and $c \in nA \cap (n+m)A$. By Lemma 6, we have

$$(h-1)c \in \bigcap_{i=0}^{h-1} ((h-1)n + im)A.$$

Since $G \setminus \left(\bigcup_{i=1}^{h} iA\right)$ is finite, we conclude that

$$m \cdot G \setminus \left(\bigcup_{i=1}^{h} miA\right)$$

is also finite. It follows that

$$(h-1)c + m \cdot G \setminus ((h-1)n + hm)A \tag{16}$$

is finite.

On the other hand, the group $G/m \cdot G$ is finite and clearly m-torsion. Also, $\langle \overline{A} - \overline{A} \rangle = G/m \cdot G$, where $\overline{A}$ is the image of A under the projection $G \to G/m \cdot G$. By Lemma 10, we have

$$sm\overline{A} = G/m \cdot G.$$

In other words, there is a system of representatives $\{x_1, \dots, x_k\}$ of $G/m \cdot G$ in G such that

$$x_j \in smA \tag{17}$$

for any $j = 1, \dots, k$.

For any $x \in G$, there exists $1 \leq j \leq k$ such that $x - (h-1)c - x_j \in m \cdot G$. It follows from (16) that for all but finitely many $x \in G$, we have

$$x - x_j \in ((h-1)n + hm)A. \tag{18}$$

By writing

$$x = x - x_j + x_j$$

and using (17) and (18), we have

$$G \sim (sm + (h-1)n + hm)A.$$

Therefore, A is a basis of order at most

$$sm + (h-1)n + hm = sm + (h-1)(m+n) + m \leq h^2 + sh + h - 1.$$

(Recall that $m + n = h + 1$.) □

Another remark is worth making here. The hypothesis of Theorem 3 is satisfied if $G/m \cdot G$ is finite for any m. Divisible groups (i.e. such that $m \cdot G = G$, for all $m \geq 1$), which include $\mathbb{R}$ and $\mathbb{Q}$, satisfy of course this property. It is easy to see that finitely generated abelian groups also satisfies this property. The group $\mathbb{Z}_p$ of p-adic integers also satisfies this property, since $\mathbb{Z}_p/m \cdot \mathbb{Z}_p \cong \mathbb{Z}/p^l \cdot \mathbb{Z}$, where p^l is the highest power of p in m. Infinite groups, all of whose proper quotients are finite, (called *just infinite* groups) satisfy this property. Note that $\mathbb{Z}_p$ is not just infinite, since $\mathbb{Z}_p/\mathbb{Z}$ is infinite.

We now turn to lower bounds and prove Theorem 4. In fact, we are able to "lift" the lower bound in (5) (applied to $\mathbb{N}$) to more general groups simply because the basis giving this example in $\mathbb{N}$ is in fact a nice basis.

Proof of Theorem 4. Let

$$g = \left\lceil \frac{h(h+4)}{3} \right\rceil + 1$$

and $k = g - 1$. According to Theorem 20 in [13], there exists a set $A \subset \mathbb{Z}/g\mathbb{Z}$ of two elements such that :

(i) $A \cup 2A \cup \cdots \cup hA = \mathbb{Z}/g\mathbb{Z}$,
(ii) $(k-1)A \neq \mathbb{Z}/g\mathbb{Z}$,
(iii) $kA = \mathbb{Z}/g\mathbb{Z}$.

Since $\mathbb{Z}$ is a quotient of G, $\mathbb{Z}/g\mathbb{Z}$ is also a quotient of G. That is, there is a subgroup K of G such that $G/K \cong \mathbb{Z}/g\mathbb{Z}$.

Let $B = \{x \in G : \overline{x} \in A\}$, where $\overline{x}$ denotes the coset of x in G/K. Then Lemma 4 implies that

(i) $B \cup 2B \cup \cdots \cup hB = G$,
(ii) $(k-1)B \neq G$,
(iii) $kB = G$.

In other words, $\mathrm{ord}^*_G(B) = k$. By (13), this implies that

$$X_G(h) \geq k = \left[\frac{h(h+4)}{3}\right].$$

□

5.2. **The torsion case.** In this section, we suppose that $px = 0$ for any $x \in G$, where p is a prime. When G is torsion, we can shorten the length of the sequence of sumsets in question, which explains the dramatically improved upper bound for $X_G(h)$.

Proof of Theorem 5 (i). Again, we use the definition (13) of X_G. Let A be any weak basis of order at most h and suppose $\mathrm{ord}^*_G(A) = k$. Since $px = 0$ for any $x \in G$, we have the inclusion $nA \subset (n+p)A$ for any n. Therefore $\cup_{i=h-p+1}^{h} A \sim G$. Lemma 5 implies that

$$\bigcup_{i=h-p+2}^{h+1} iA = G. \tag{19}$$

Clearly, we also have

$$\bigcup_{i=h-p+3}^{h+2} iA = G. \tag{20}$$

We now distinguish two cases.

Case 1: $(h+2)A \cap nA = \emptyset$, for any $h-p+3 \leq n \leq h+1$. Then from (19) and (20), and since $(h-p+2)A \subset (h+2)A$, we have necessarily

$$(h-p+2)A = (h+2)A.$$

By repeatedly adding pA to both sides, we have

$$(h-p+2)A = (h+2+lp)A$$

for any $l \geq 0$. If l is sufficiently large then $h+2+lp \geq k$ and $(h+2+lp)A = G$. Therefore, $(h-p+2)A = G$ and $k \leq h-p+2 \leq h$.

Case 2: $nA \cap (h+2)A \neq \emptyset$ for some $h-p+3 \leq n \leq h+1$. Put $m = h+2-n$. We argue as in the beginning of the proof of Theorem 3. If $c \in nA \cap (n+m)A$, then by Lemma 6, we have

$$(p-1)c \in \bigcap_{i=0}^{p-1} ((p-1)n + im)A. \tag{21}$$

Next we claim that

$$\bigcup_{i=h-p+1}^{h} iA \subset \bigcup_{i=0}^{p-1} (h-p+1+im)A.$$

Indeed, since $(m,p)=1$, $\{im\}_{i=0}^{p-1}$ forms a complete residue system modulo p. If j is the least nonnegative residue of im modulo p, then $im \equiv j \pmod p$ and $im \geq j$, so that

$$(h-p+1+im)A \supset (h-p+1+j)A.$$

Therefore,

$$G \sim \bigcup_{i=0}^{p-1} (h-p+1+im)A.$$

For all but finitely many $x \in G$, we have

$$x-(p-1)c \in \bigcup_{i=0}^{p-1} (h-p+1+im)A. \tag{22}$$

Combining (22) and (21) we see that for all but finitely many $x \in G$

$$\begin{aligned} x &\in ((h-p+1)+(p-1)m+(p-1)n)\,A \\ &= (h-p+1+(p-1)(h+2))A = (hp+p-1)A. \end{aligned}$$

Therefore, $\mathrm{ord}_G^*(A) \leq hp+p-1$. □

In order to find a lower bound for $X_G(h)$ we use the same idea as in Theorem 4, namely, to find a nice basis in a quotient of G. Note that G is an infinite vector space over $\mathbb{F}_p$. Consequently, all finite quotients of G are isomorphic to $\mathbb{F}_p^d$, for some d. Nice weak bases of cardinality d in $\mathbb{F}_p^d$ are very well understood by the following:

Lemma 11. *Let $A=\{e_1,\dots,e_d\} \subset \mathbb{F}_p^d$. Then A is a nice weak basis of $\mathbb{F}_p^d$ if and only if $e_1,\dots,e_d$ are linearly independent. If this condition is satisfied, then every element in $\mathbb{F}_p^d$ can be expressed as a sum of $\leq (p-1)d$ elements from A, and $(p-1)d$ is best possible.*

Proof. Clearly $iA \in \langle A\rangle$ for any i. If A is a nice weak basis, then necessarily $\langle A\rangle = \mathbb{F}_p^d$ and consequently $e_1,\dots,e_d$ are linearly independent. Suppose that $e_1,\dots,e_d$ are linearly independent. For any $0 \leq \alpha_1,\dots,\alpha_d \leq p-1$, the element $\sum_{i=1}^d \alpha_i e_i$ is a sum of $\sum_{i=1}^d \alpha_i \leq (p-1)d$ elements from A. Furthermore, $\sum_{i=1}^d (p-1)e_i$ cannot be expressed as a sum of fewer than $(p-1)d$ elements from A. □

This leads us to the following characterization of nice bases of cardinality $d+1$ in $\mathbb{F}_p^d$.

Lemma 12. *Let $A=\{e_1,\cdots,e_d,\alpha_1e_1+\cdots+\alpha_de_d\} \subset \mathbb{F}_p^d$, where $e_1,\dots,e_d$ are linearly independent. Then A is nice basis of $\mathbb{F}_p^d$ if and only if*

$$\sum_{i=1}^d \alpha_i \not\equiv 1 \bmod p.$$

If this condition is satisfied, then $d(p-1)A=\mathbb{F}_p^d$ and $(d(p-1)-1)A \neq \mathbb{F}_p^d$.

Proof. We make the simple yet crucial observation that A is a nice basis if and only if $A-a$ is a nice basis (Lemma 1). (Note that this property fails for *vector space bases.*) We have

$$A-e_1 = \{0, e_2-e_1,\cdots,e_d-e_1,(\alpha_1-1)e_1+\cdots+\alpha_de_d\}.$$

Clearly, $(A-e_1)$ is a nice basis if and only if $(A-e_1)\setminus\{0\}$ is a nice weak basis. By Lemma 11, we only need to check when $(A-e_1)\setminus\{0\}$ is a family of d independent vectors. In the vector space basis $\{e_1,\dots,e_d\}$, we have

$$\begin{aligned}\det(\{e_2-e_1,\cdots,e_d-e_1,(\alpha_1-1)e_1+\cdots+\alpha_de_d\})&\\ =\begin{vmatrix} -1 & -1 & \cdots & \cdots & -1 & -1 & \alpha_1-1\\ 1 & 0 & \cdots & \cdots & 0 & 0 & \alpha_2\\ 0 & 1 & 0 & \cdots & 0 & 0 & \alpha_3\\ 0 & 0 & 1 & \ddots & \cdots & \vdots & \vdots\\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots & \vdots\\ \vdots & \vdots & & \ddots & 1 & 0 & \vdots\\ 0 & 0 & \cdots & \cdots & 0 & 1 & \alpha_d \end{vmatrix}&\\ =\sum_{i=1}^{d}\alpha_i-1,&\end{aligned}$$

and the first part of Lemma 12 follows. The second part of Lemma 12 follows from the second part of Lemma 11. □

We can now construct a nice basis in $\mathbb{F}_p^d$ which plays a similar role to the set A used in the proof of Theorem 4.

Lemma 13. *Let $e_1,\cdots,e_d$ be d linearly independent vectors in $\mathbb{F}_p^d$. Suppose that $d\not\equiv 1 \bmod p$. Then the set*

$$A=\{e_1,\cdots,e_d,e_1+\cdots+e_d\}$$

satisfies the following properties:

(i) *any element in $\mathbb{F}_p^d$ can be expressed as a sum of at most $(d+1)(p-1)/2$ elements from A,*
(ii) $(d(p-1)-1)A\neq\mathbb{F}_p^d$,
(iii) $d(p-1)A=\mathbb{F}_p^d$.

Proof. The last two assertions follow directly from Lemma 12 and the assumption that $d\not\equiv 1 \bmod p$.

As for the first one, put $a=\sum_{i=1}^{d}e_i$. Consider an arbitrary element $x=x_1e_1+\cdots+x_de_d\in\mathbb{F}_p^d$. Define

$$\alpha_i=\left|\{x_j\equiv i \bmod p\}\right|.$$

For all $0\le i\le p-1$, we can write

$$x=ia+\sum_{j=1}^{d}(x_j-i)e_j=ia+\sum_{j=1}^{d}y_je_i$$

with $0\le y_j\le p-1$. In this decomposition of x, we use $i+\alpha_{i+1}+2\alpha_{i+2}+\cdots+(p-1)\alpha_{i+p-1}$ elements of A. Thus, x can be written using

$$\min_i\{i+\alpha_{i+1}+2\alpha_{i+2}+\cdots+(p-1)\alpha_{i+p-1}\}$$

elements of A.

Since

$$\sum_{i=0}^{p-1}(i+\alpha_{i+1}+2\alpha_{i+2}+\cdots+(p-1)\alpha_{i+p-1}) = \left(\sum_{i=0}^{p-1}\alpha_i\right)\frac{p(p-1)}{2}+\frac{p(p-1)}{2}$$
$$= (d+1)\,\frac{p(p-1)}{2}$$

the minimum among the i's is at most $(d+1)(p-1)/2$, which proves the first assertion of Lemma 13. □

Proof of Theorem 5 (ii). If $[2h/(p-1)-1] \not\equiv 1 \bmod p$, let

$$d = \left[\frac{2h}{p-1}-1\right].$$

If not, we choose

$$d = \left[\frac{2h}{p-1}-2\right].$$

Since $h \geq 3(p-1)/2$, we have $d \geq 1$.

We now proceed as in the proof of Theorem 4. Let $A \subset \mathbb{F}_p^d$ be the set given by Lemma 13. Since $(d+1)(p-1)/2 \leq h$, we have

(i) $A \cup 2A \cup \cdots \cup hA = \mathbb{F}_p^d$,
(ii) $(d(p-1)-1)A \neq \mathbb{F}_p^d$,
(iii) $d(p-1)A = \mathbb{F}_p^d$.

There is a subgroup K of G such that $G/K \cong \mathbb{F}_p^d$. Let $B = \{x \in G : \overline{x} \in A\}$, where $\overline{x}$ denotes the coset of x in G/K. Lemma 4 implies that

(i) $B \cup 2B \cup \cdots \cup hB = G$,
(ii) $(d(p-1)-1)B \neq G$,
(iii) $d(p-1)B = G$.

This implies that

$$X_G(h) \geq \mathrm{ord}_G^*(B) = d(p-1) \geq (p-1)\left(\frac{2h}{p-1}-3\right) = 2h-3p+3.$$

□

We notice that the proof shows that we have a better bound $X_G(h) \geq 2h-2p+2$ in the case $d = [2h/(p-1)-1] \not\equiv 1 \bmod p$. Also, if $p=2$, then Theorem 5 (i) and the proof of Theorem 5 (ii) imply the rather tight bounds, namely

$$2h-2 \leq X_{\mathbb{F}_2[t]}(h) \leq 2h+1.$$

It is perhaps of interest to determine the exact value of $X_G(h)$ when $p=2$.

5.3. **When h is small.** In this section we prove Theorem 6. Note that the lower bounds $X_G(2) \geq 3$ and $X_G(3) \geq 4$ are immediate consequences of Theorem 1. In proving the upper bounds, we again use the definition (13) of X_G.

Proof of Theorem 6(i). Suppose

$$A \cup 2A \sim G$$

and $\mathrm{ord}^*_G(A) = k$ is finite. By Lemma 5, for every $l \geq 2$, we have

$$lA \cup (l+1)A = G.$$

Case 1: There exists c in $2A \cap 3A$. For all but finitely many $x \in G$, we have $x - c \in A \cup 2A$. Thus for all but but finitely many $x \in G$, $x = x - c + c \in 4A$, and $4A \sim G$.

Case 2: $2A \cap 3A = \emptyset$. If there exists $c \in 3A \cap 4A$, then by the same argument as above, we have $5A \sim G$. Let us assume that $3A \cap 4A = \emptyset$. Since $2A \cup 3A = 3A \cup 4A = G$, we deduce $2A = 4A$. It follows that $2A = 2mA$ for all $m \geq 1$. If $2m > k$ then $2mA = G$ and $2A = G$.

In any case we have $\mathrm{ord}^*_G(A) \leq 5$. □

Proof of Theorem 6(ii). Suppose

$$A \cup 2A \cup 3A \sim G$$

and $\mathrm{ord}^*_G(A) = k$ is finite. By Lemma 5, for every $l \geq 2$, we have

$$lA \cup (l+1)A \cup (l+2)A = G.$$

Observe that if $iA \cap (i+1)A \neq \emptyset$, then $2iA \cap (2i+1)A \cap (2i+2)A \neq \emptyset$ and this implies $(2i+3)A \sim G$. Thus we can assume that $iA \cap (i+1)A = \emptyset$ for $1 \leq i \leq 7$. Otherwise, $\mathrm{ord}^*(A) \leq 2i + 3 \leq 17$. We distinguish three cases.

Case 1: $0 \in 2A$. Then $4A \supset 2A$ and $5A \supset 3A$. It follows that $3A \cup 4A = G = 4A \cup 5A$. By assumption, these are partitions of G. Therefore, $3A = 5A$, which implies $3A = (2m+3)A$ for any $m \geq 1$. Consequently, $3A = G$ and $\mathrm{ord}^*_G(A) \leq 3$.

Case 2: $0 \in 3A$. Then $5A \supset 2A$ and $6A \supset 3A$. Since $5A \cap 6A = \emptyset$, $5A \cap 3A = \emptyset$. Thus, $3A \cup 4A \cup 5A = G$ is a partition of G. On the other hand, since $2A \cup 3A \cup 4A = G$, we deduce that $2A = 5A$ Similarly to the previous case, we have $\mathrm{ord}^*_G(A) \leq 2$.

Case 3: $0 \in 4A$. Then $6A \supset 2A$, $7A \supset 3A$, $8A \supset 4A$, and $2A \cup 3A \cup 4A = G = 6A \cup 7A \cup 8A = G$. Since $7A$ is disjoint from $6A$ and $8A$, we deduce $3A = 7A$. Similarly to the previous case, we have $\mathrm{ord}^*_G(A) \leq 3$. □

6. The function S_G

The key in generalizing Cassaigne and Plagne's argument [2] is the notion of *amenability*. Among the many equivalent definitions of amenability, we work with the one defined in terms of *invariant means*. Let G be a discrete (not necessarily abelian) group. Let $l^\infty(G)$ denote the set of all bounded functions on G. A right-invariant mean on G is a linear functional $\Lambda : l^\infty(G) \to \mathbb{R}$ satisfying:

(i) Λ is nonnegative: if $f \geq 0$ on G, then $\Lambda(f) \geq 0$,
(ii) Λ has norm 1: $\Lambda(1_G) = 1$ where 1_G is the characteristic function of G,
(iii) Λ is right-invariant: $\Lambda(\tau_g f) = \Lambda(f)$ for any $f \in l^\infty(G)$ and $g \in G$, where τ_g is the right translation: $\tau_g f(x) = f(xg)$.

G is called *amenable* if there exists a right-invariant mean on G.

We recall here some standard facts about amenable groups. For a reference, see for example [1, Appendix G]. The additive group of the integers $\mathbb{Z}$ is amenable. The existence of invariant means on $\mathbb{Z}$ is non-constructive, since it requires either the use of ultrafilters or the Hahn-Banach theorem. More generally, any discrete abelian group is amenable. The free subgroups on two generators is not amenable.

Proof of Theorem 7. The lower bound $h + 1 \leq S_G(h)$ is an immediate consequence of Theorem 1. We will now prove the upper bound. Let Λ be an invariant mean on G. Since G is infinite, it is easy to see that $\Lambda(1_I) = 0$ for all finite subset $I \subset G$, where 1_I is the characteristic function of I (it suffices to see this for a singleton).

Let A be a basis of order h of G. Without loss of generality, we may assume that $0 \in A$.

For each element $a \in A$, let f_a be the function on G defined by

$$f_a(x) = \begin{cases} 1, & \text{if } x \in hA \setminus h\,(A \setminus \{a\}) \\ 0, & \text{otherwise.} \end{cases}$$

In other words, $f_a(x) = 1$ if and only if a is essential in all representations of x as a sum of h elements from A.

Just like in the proof given in [2], we make two observations. First, for any $x \in G$ and finite subset $I \subset A$, we have $\sum_{a \in I} f_a(x) \leq h$. Indeed, if $x \notin hA$ clearly then $f_a(x) = 0$ for any $a \in A$. Suppose $x \in hA$. Fix a representation

$$x = a_1 + \cdots + a_h$$

where $a_i \in A$. Then $f_a(x)$ can only be 1 if a is one of the a_i, and there are at most h of these.

Applying Λ to both sides, we have proved the following statement.

Claim 1. *For any finite subset $I \subset A$, we have*

$$\sum_{a \in I} \Lambda(f_a) \leq h.$$

Our next claim is this :

Claim 2. *If $a \in A$ is such that $\Lambda(f_a) < 1/h$, then there exists $x \in G$ such that*

$$x + ia \in h(A \setminus \{a\})$$

for any $i = 0, 1, \ldots, h-1$.

Indeed, since Λ is translation invariant, we have

$$1 > h\Lambda(f_a) = \sum_{i=0}^{h-1} \Lambda\left(\tau_{ia} f_a\right) = \Lambda\left(\sum_{i=0}^{h-1} \tau_{ia} f_a\right).$$

It follows that for an infinite set $B \subset G$, we have

$$1 > \sum_{i=0}^{h-1} \tau_{ia} f_a(x) = \sum_{i=0}^{h-1} f_a(x + ia).$$

for all $x \in B$. Consequently, for any $x \in B$, $f_a(x + ia) = 0$ for any $i = 0, 1, \ldots, h-1$.

Since $hA \sim G$, there must exist such an $x \in B$ such that $x + ia \in hA$ for any $i = 0, 1, \ldots, h-1$. For this x, we have

$$x + ia \in h(A \setminus \{a\})$$

for any $i = 0, 1, \ldots, h-1$, as required.

From Claim 1 it follows that for all but finitely many $a \in A$, we have $a \neq 0$ and $\Lambda(f_a) < 1/h$. For such an a, let x be such that $x + ia \in h(A \setminus \{a\})$ for any $i = 0, 1, \ldots, h-1$, whose existence is given by Claim 2. Now for all but finitely many $y \in G$, we have $y - x \in hA$ and $y - x \neq ha$. By removing any occurrence of a, it follows that for some $0 \leq i \leq h-1$, we have

$$y - x - ia \in (h - i)(A \setminus \{a\}).$$

This implies that

$$y = (y - x - ia) + (x + ia) \in (2h - i)(A \setminus \{a\}) \subset 2h(A \setminus \{a\})$$

which proves that $A \setminus \{a\}$ is a basis of order at most $2h$. □

Notice that the definition of amenability can be extended to locally compact groups. The definition is the same, except that we replace $l^\infty(G)$ by $L^\infty(G, \mu)$ where μ is a Haar measure on G. Again, it is known that all abelian locally compact groups are amenable. The argument above can be applied to these groups as well, with an appropriate change in the definition of order. Instead of requiring $hA \sim G$, we require $\mu(G \setminus hA) = 0$.

Proof of Theorem 8. Since $S_G(2) \geq 3$, it suffices to show that $S_G(2) \leq 3$. Let A be a basis of order at most 2 of G. Call $b \in A$ *bad* if $\mathrm{ord}^*(A \setminus \{b\}) \geq 4$ and *good* otherwise. We will show that A has only finitely many bad elements.

By considering $A - c$ instead of A where c is any element of A, we may assume that $0 \in A$.

We first examine properties of a bad element $b \in A, b \neq 0$. Let us write $A_b = A \setminus \{b\}$. Since A is a basis of order 2, we have

$$G \sim 2A \sim 2A_b \cup (A_b + b). \tag{23}$$

Let a be an arbitrary element of A_b. Then

$$G \sim 2A + a \sim (2A_b + a) \cup (A_b + b + a) \subset 3A_b \cup (A_b + b + a). \tag{24}$$

From (23) we also deduce

$$G \sim 2A_b \cup (A_b + b) \subset 3A_b \cup (A_b + b). \tag{25}$$

From (24) and (25) we see that the sets $(A_b + b + a)$ and $(A_b + b)$ both contain all but finitely many elements of $G \setminus 3A_b$. Since b is bad, this implies that $(A_b + b + a) \cap (A_b + b)$ is infinite. In other words, we have proved:

Claim 1: For any $a \in A_b$, $(A_b + a) \cap A_b$ is infinite.

Next we prove

Claim 2: $(A_b + b) \cap A_b = \emptyset$.

Indeed, suppose for a contradiction that there are $a_1, a_2 \in A_b$ such that $b + a_1 = a_2$. For all but finitely many $x \in A$, we have $x - a_1 \in 2A \setminus \{2b\}$. If $x - a_1 \in 2A_b$ then $x \in 3A_b$. If $x - a_1 \in A_b + b$ then $x \in A_b + a_2 \subset 2A_b \subset 3A_b$. Thus $3A_b \sim G$, a contradiction.

Suppose now that there is another bad element $b' \in A, b' \neq 0$. From Claim 1 we know that $(A_b + b') \cap A_b$ is infinite. Therefore, $(A \setminus \{b, b'\} + b') \cap (A \setminus \{b, b'\})$ is infinite. But this contradicts Claim 2 (with b replaced by b'). □

In fact, the proof shows that there is at most one bad element in A. Indeed, the above argument shows that for any $c \in A$, there is at most one bad element in A that is different from c. Applying this observation to a good element c (which we know to exist), this implies that there is at most one bad element in A.

Acknowledgements

The authors are supported by the ANR grant Cæsar, number ANR 12-BS01-0011. The second author is supported by the Fondation Mathématique Jacques Hadamard. We would like to thank P. Longobardi and M. Maj for a useful discussion.

References

[1] B. Bekka, P. de la Harpe, A. Valette, Kazhdan's Property (T), New Mathematical Monographs 11, Cambridge University Press, Cambridge, 2008.
[2] J. Cassaigne, A. Plagne, *Grekos' S function has a linear growth*, Proc. Amer. Math. Soc. **132** (2004), 2833–2840.
[3] P. Erdős, R. L. Graham, *On bases with an exact order*, Acta Arith. **37** (1980), 201–207.
[4] P. Erdős, R. L. Graham, Old and new problems and results in combinatorial number theory, Monogr. Enseign. Math. 28, 1980.
[5] G. Grekos, *Extremal problems about asymptotic bases: a survey*, Combinatorial number theory, 237–242, de Gruyter, Berlin, 2007.
[6] G. Grekos, *Sur l'ordre d'une base additive*, Séminaire de Théorie des Nombres de Bordeaux (Talence, 1987–1988), Exp. No. 31, 13 pp.
[7] G. Grekos, *Extremal problems about additive bases*, Acta Math. Inform. Univ. Ostraviensis **6** (1998), no. 1, 87–92.
[8] G. Grekos, *Minimal additive bases and related problems*, Number theory days, 1980 (Exeter, 1980), 300–305, London Math. Soc. Lecture Note Ser., 56, Cambridge Univ. Press, Cambridge, 1982.
[9] E. Härtter, *Ein Beitrag zur Theorie der Minimalbasen*, J. Reine Angew. Math. **196** (1956), 170–204.
[10] M. B. Nathanson, *Minimal bases and powers of 2*, Acta Arith. **49** (1988), 525–532.
[11] J. C. M. Nash, *Some applications of a theorem of M. Kneser*, J. Number Theory **44** (1993), 1–8.
[12] A. Plagne, *Problemas combinatorios sobre bases aditivas*, Gac. R. Soc. Mat. Esp.**9** (2006), 191–201.

[13] A. Plagne, *À propos de la fonction X d'Erdős et Graham*, Ann. Inst. Fourier (Grenoble) **54** (2004), no. 6, 1717–1767.
[14] A. Plagne, *Sur le nombre d'éléments exceptionnels d'une base additive*, J. Reine Angew. Math. **616** (2008), 47–65.
[15] A. Stöhr, *Gelöste und ungelöste Fragen über Basen der natürlichen Zahlenreihe I, II*, J. Reine Angew. Math. **194** (1955), 40–65 and 111–140.

Centre de Mathématiques Laurent Schwartz, École polytechnique, 91128 Palaiseau Cedex, France

E-mail address: victor.lambert@ens-cachan.org

E-mail address: thai-hoang.le@polytechnique.edu

E-mail address: plagne@math.polytechnique.fr